Federal eDiscovery Rules Update: Recent Cases Applying The New Amendments

John Patzakis

July 12, 2007

Agenda

- Recent eDiscovery Case Law Update
- Preservation and Collection Best Practices
- Resources and Q&A

Recent Process Scrutiny Case: Google v. American Blind

Google Inc. v. Am. Blind & Wallpaper Factory, Inc., 2007 WL 1848665 (N.D. Cal. June 27, 2007)

- Google alleges American Blind made inadequate efforts to preserve, collect, and produce relevant evidence.
- American Blind Asserted That Preservation Notices Were Sent to Custodians
- Court ordered American Blind to provide declarations stating "what they ***did*** with respect to preserving and collecting documents." (emphasis in original)
- Court Determines that "no concerted effort was made to search for internal email" and that the "record demonstrates a willful indifference at American Blind towards ensuring that relevant documents were preserved, collected and produced."
- Severe Evidentiary Sanctions and $15,000 in monetary sanctions imposed.

Court Scrutiny of E-Discovery Collection Process Litigation Hold Memos Are Not Enough

Due diligence is required:

- *In re NTL, Inc. Securities Litigation,* 2007 WL 241344 (S.D.N.Y. Jan. 30 2007)
  - "Although NTL sent out hold memos in March and June 2002 . . . those hold memos were not sufficient, since they subsequently were ignored by both NTLs. . . . The evidence, in fact, is that no adequate litigation hold existed at the NTLs."" (*16, citing *Zubulake*).
- *Samsung Electronics v. Rambus,* 439 F.Supp.2d 524 (E.D. Va. 2006)
  - "It is not sufficient, however, for a company merely to tell employees to 'save relevant documents,' ... this sort of token effort will hardly ever suffice."
  - court faults "the lack of specificity in defining what documents would be relevant to litigation"
- *Wachtel v. HealthNet*, 2006 WL 3538935 (D.N.J.); Court criticizes HealthNet's "utterly inadequate" eDiscovery process where paralegal merely emails preservation notifications

Would Your Organization's eDiscovery Search and Collection Efforts Withstand This Scrutiny?

- *Peskoff v. Ferber* 240 F.R.D. 26 (2007, D.D.C.)

  "Once the search is completed...Defendant must also file a statement under oath by the person who conducts the search, **explaining how the search was conducted**, of which electronic depositories, **and how it was designed to produce and did in fact produce all of the emails I have just described**. I must insist that the person performing the search have the **competence and skill to do so comprehensively**. An evidentiary hearing will then be held, at which I expect the person who made the attestation **to testify and explain how he or she conducted the search**, his or her qualifications to conduct the search, and why I should find the search was adequate."

- At Such "Process Defense" Hearings Parties Will be Best Served By Pointing to Best Practices Processes and Technology instead of *ad hoc* self-collection.

The Initial Disclosure Rules 26(a) & (f)

- Key Guidance From New Judicial Handbook:

"All too often, attorneys view their obligation to 'meet and confer' under Federal Rule of Civil Procedure 26(f) as a perfunctory exercise. When ESI is involved, judges should insist that a meaningful Rule 26(f) conference take place and that a meaningful discovery plan be submitted."

--*Managing Discovery of Electronic Information*: *A Pocket Guide for Judges*; Federal Judicial Center, 2007

Know Thyself: Early Attention and Systemization

- At Outset of Case, Counsel Must Understand Information Systems Architecture and Where Relevant ESI is Located.
- See, *Phoenix Four v. Strategic Resources Group* 2006 WL 1409413 (S.D.N.Y) (Sanctions for failure to produce relevant ESI from unmapped server partition)
  - Applies Federal Rule Amendments
- *Caveat*: Many Other Potential Issues: Admin. Level Encryption, Multiple Storage Points Per Custodian
- IT Persons Most Knowledgeable Must Be Identified.

  -Committee Notes to 26(f)
- Conclusion: A Pre-Established and Systemized Identification and Preservation Process Must Be in Place

Search Strategy: The Manual for Complex Litigation Tie In To Rule 26(f)

- Rule 26(f) Committee Notes Cite Manual for Complex Litigation (MCL) (4th) §40.25 (2):
  - The particular issues regarding electronically stored information that deserve attention during the discovery planning stage depend on the specifics of the given case. See Manual for Complex Litigation (4th) § 40.25(2) (listing topics for discussion in a proposed order regarding meet-and-confer sessions).
- MCL 40.25(2) States: "The parties should attempt to reach agreement on all issues regarding the preservation of documents, **data**, and tangible things. These issues include…:

  (a) the extent of the preservation obligation, identifying the types of material to be preserved, the subject matter, time frame, the authors … and ***key words*** to be used in identifying responsive materials"

Several Recent Cases Support Targeted and Narrow ESI Search and Collection Strategy

- "Clearly [there is no duty to] preserve every shred of paper, every e-mail or electronic document, and every backup tape…Such a rule would cripple large corporations." *Zubulake v. UBS Warburg LLC,* 220 F.R.D. 212, 217 (S.D.N.Y. 2004) ("*Zubulake IV*")

- *In re Genetically Modified Rice Litigation*, 2007 WL 1655757 (June 5, 2007 E.D.Mo.)
  - "Preservation efforts can become unduly burdensome and unreasonably costly unless those efforts are targeted to those documents reasonably likely to be relevant or lead to the discovery of relevant evidence related to the issues in this matter."
- *Treppel v. Biovail Corporation*, 233 F.R.D. 363 (S.D.N.Y. 2006).
  - Court: defined search strategies are appropriate in cases involving ESI. If meet and confer efforts are refused, producing party should proceed with reasonable search criteria with a clear record of opponent's refusal.
- *Caveat*: Without an Established Process with the Right Technology, Collection Efforts Will Be Overly Broad, Resulting in Substantial "Back End" Costs (processing, excess data hosting and review).

Authentication of Electronic Evidence: *Lorraine v. Markel* --- F.R.D. ----, 2007 WL 1300739 (D.Md.)

- Federal District Court Case in Maryland. Motions for Summary Judgment Denied Because They Failed to Properly Authenticate the Computer Evidence.
- Judge notes the lack of "comprehensive analysis of the many interrelated evidentiary issues associated with electronic evidence," sets off to undertake "a broader and more detailed analysis of these issues."
- Does Not Require Deep Dive Forensics, but Notes the Importance of Proper Collection, and Evidence Handling
- Key Issues: Importance of Metadata, Hash Values, Automated and Defendable Collection Processes

Safe Harbor: Only Possible with a Process

- Rule 37(f): No Penalties for Deleting ESI due to ***Routine*** Operation of IT Systems, and if Reasonable Preservation Steps Taken
- Must be Due to ***Routine Operation*** and in ***Good Faith***
  - Procedures Must be: Established, Documented and Operational
  - Systemized Framework For Early Attention (Litigation Hold) Must be in Place
  - Caveat --- Committee Note: “A party is not permitted to exploit the routine operation of an information system to thwart discovery obligations by allowing that operation to continue in order to destroy (relevant ESI).”

Rule 34(b) "Native File Production" Provision: Defensible Collection Required

- Rule 34(b): Permits Requesting Party to Specify the Form it Wants the ESI to be Produced
- Key Comments to Rule 34(b):
  - "The form of production is more important to the exchange of electronically stored information than of hard-copy materials."
  - If ESI is ordinarily stored in searchable format, it "should not be produced in a form that removes or significantly degrades this feature."
- Note: Many Recent Cases re Metadata;
  - *Nova Measuring Instruments Ltd. v. Nanometrics, Inc.,* 417 F.Supp.2d 1121 (2006 N.D.Cal); ("[a party] must produce the documents in their native file format, with original metadata.")
- **Conclusion:** Without Best Practices Tools and Processes, ESI Metadata and Native Format Will Likely be Lost or Altered

10 Common Pitfalls That Reduce Defensibility and Increase Costs of Legal Holds

1. Lack of a repeatable process
2. Inconsistent or ad hoc litigation hold team membership
3. Failure to document all steps and decisions taken
4. Copying documents using methods that affect metadata
5. Inadequate attention to chain of custody

10 Common Legal Hold Pitfalls (cont'd)

6. Relying on legal hold notices alone for preservation
7. Relying on custodians to identify and/or collect responsive files and emails
8. Not Utilizing Technology Designed for eDiscovery (ie IT Storage Backup)
9. Collection Methodology Does Not Integrate with Processing and Review
10. Overcollection – increases cost and adds complexities (indicator of no or poorly defined process)

About Guidance Software

- Founded 1997. (NASD: GUID)
- Largest provider of computer investigation software, training and services
  - Over 25,000 users of EnCase® computer forensic software worldwide
  - More than 3,800 trained annually
  - Customers:
    - Major federal government agencies
    - Over 370 of Global 2000, including over 100 of the Fortune 500, use EnCase® Enterprise software
- Headquartered in Pasadena, CA
    - Offices in SF, DC, NY, Houston, Chicago (opening Q1 2007) and the UK

...Coupled with its Proven Track Record and Court Credibility

- EnCase Validated Under Daubert/Frye. For example:
  - *Sanders v. State (Texas)*, 191 S.W. 3rd 272 (Tex.App., 2006); *Cert. Denied*, 127 S.Ct. 1141, 166 L.Ed.2d 893 (U.S.) (Court takes Judicial Notice of the reliability of EnCase, finding "**EnCase is a 'field standard' for forensic computer examination**.")
  - *Krumwiede v. Brighton Assocs., L.L.C.,* 2006 WL 1308629 (N.D. Ill. May 8, 2006) [Court finds that eDiscovery Consultant "created a forensically valid copy of the laptop's hard drive using EnCase software." This allowed the consultant "to examine the metadata and the content of the files on the computer..."]
  - *Williford v. State (Texas),* 127 S.W.3d 309 (Tex.App. 2004).
  - *State (Ohio) v. Cook*, 777 N.E.2d 882 (Ohio App. 2002)
- Used by the SEC, FBI, Secret Service, FTC, foreign governments, state and local law enforcement, etc.
  - *See, e.g., United States v. Shirazi,* 2006 WL 1155945 (N.D.Ill., May 1, 2006) (FBI affidavit specifically points to its use of EnCase to justify search and seizure of computers)

Further Resources

Request Copy of Amended FRCP and new white paper:
Legal@guidancesoftware.com

Detailed White Papers:
www.guidancesoftware.com/commercial/legalresources.asp

eDiscovery Resources:
www.kenwithers.com
www.thesedonaconference.org

The Discovery Revolution “E-Discovery Amendments to the Federal Rules of Civil Procedure”, George Paul and Bruce Nearon; ABA Publishing, 2006
www.ababooks.org

“Digital Discovery & e-Evidence” Pike & Fisher
http://ddee.pf.com